Amendments to the Specification:

Please replace the paragraph beginning at page 11, line 14, which begins "In network environments using Dynamic Host Configuration Protocol" with the following amended paragraph:

In network environments using Dynamic Host Configuration Protocol (DHCP), IP addresses are automatically assigned to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers. In DHCP environments, the ~~ARPc ache~~ ARP cache maintains lease times on assigned IP addresses of up to four days for a direct connection. For dial-up connections, the DHCP lease time of the IP address is often less than an hour. Then, at step 306, the ARP cache of the network router that is known to have transmitted network traffic for the missing device is searched. The device's hostname or IP address will index within the ARP cache to previous data packet transmissions of the network device. From the data packets, ~~an~~ a unique hardware fingerprint of the lost or stolen network device is extracted--such as the MAC address of the network adapter card contained within the missing device. If the device is reporting missing after a significant period time since its last access to the Internet, the ARP cache may have been flushed. In this case, the process would obtain the hardware fingerprint of the missing device through an alternative method. For example, previous emails sent from the missing device or other artifacts sent over the network can be extracted from other receiving network machines, and then the device's MAC address or other hardware fingerprint can be extracted therefrom.

Please replace the paragraph beginning at page 13, line 1, which begins "Once the network server is alerted" with the following amended paragraph:

Once the network server is alerted that the missing machine has been used on the network, the rest of the network enveloping information in the missing machine's Internet traffic is used to attempt to isolate the computer's location. The intercepted data packets are decompiled and are used to trace the route through which the data has traveled and to extract the IP address from which they originated. In accordance with the preferred embodiment, when a match is discovered in the Internet traffic for the hardware fingerprint of a device listed in the missing equipment database, a tracing software routine is initiated in a network server that determines the Internet communication links that were used to connect the missing network device to the network server. These Internet communication links will assist the network server in tracking the network device and obtaining its IP address. The IP address of the source, of ~~an~~ a DNS query is sent to the host within the DNS query that starts the intercepted network traffic. However, if the source of the query is transmitted through a "proxy" server, then the IP address of the client computer (which may not be unique since it may not have been assigned by the InterNIC) will likely be insufficient to track the location of the client computer. In such a scenario, it is necessary to determine the addresses of other IP routers which were accessed to enable communication between the client and the host. These addresses and the times that they were accessed are compared with internal logs of the proxy server which record its clients' Internet access history. In this way, the client can be uniquely identified and located.